UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/743,796	12/24/2003	Leland A. Wallace	P3127-939	9789

21839 7590 01/09/2009
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER	
GERGISO, TECHANE	

ART UNIT	PAPER NUMBER
2437	

NOTIFICATION DATE	DELIVERY MODE
01/09/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ADIPFDD@bipc.com

Office Action Summary	Application No.	Applicant(s)	
	10/743,796	WALLACE ET AL.	
	Examiner	Art Unit	
	TECHANE J. GERGISO	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 September 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-44 and 48-51* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *13-44 and 48* is/are allowed.

6)☒ Claim(s) *1-12 and 49-51* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on September 12, 2008 has been entered.

Response to Arguments

2. Applicant's arguments with respect to claims 1-12 and 49-51 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-12 and 49-51 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kumar et al. (Hereinafter referred to as Kumar, US Pat. No.: 7, 024, 695) in view of Funk (US Pat. No.: 7, 363, 500) and in further view of Haverinen (US Pub. No. : 2004/0078571).

As per claim 1:

Kumar discloses a method for authenticating a computing device, the method comprising the following steps:

issuing a credential based on session information, a hash seed and credential information from a first computing device to a second computer computing device (column 5: lines 2-14);

transmitting said credential and a computer challenge from the second computer computing device to the first computer computing device when the second computing device is to be authenticated (column 5: lines 2-14; column 6: lines 45-65; Figure 5: server challenge; Client DPC authentication challenge response);

transmitting a response to said computer challenge from said first computer computing device to said second computer computing device (column 6: lines 55-65; column 7: lines 1-13; Figure 5: challenge response); and

verifying said response with said second computer computing device in order to authenticate and verify said computers computing devices (column 7: lines 30-40; Figure 5: Authentication response; DPC command response; success/Failure).

Kumar does not explicitly disclose credential based on a maximum iterative value security parameters. Funk in analogous art, however discloses, credential based on a maximum iterative value security parameters (column 4: lines 10-24; column 7: lines 37-42; column 18: lines 35-65). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Kumar to include credential based on a maximum iterative value security parameters. This modification would have been

obvious because a person having ordinary skill in the art would have been motivated to do so to provide secure authentication against man in the middle attack for inner protocols that can generate encryption keys as suggested by Funk in (column 5: lines 25-33).

Kumar and Funk do not explicitly disclose credential based on an expiration time. Haverinen in analogous art, however discloses, credential based on an expiration time (0022; 0035; 0036). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Kumar and Funk to include credential based on an expiration time This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide a strong authentication including Kerberos authentication service desirable in transactions involving confidential data as suggested by Haverinen (0002-0003).

As per claim 7:

Kumar discloses a system for authenticating a computer, the system comprising:

a first computer (figure 5: client); and

a second computer in communication with the first computer (figure 5: server);

wherein the first computer and the second computer are configured to execute the following instructions (Figure 5: Authentication and data integrity protocol):

issuing a credential based on session information, a hash seed, credential information from a first computing device to a second computer computing device (column 5: lines 2-14);

transmit the credential and a challenge from the second computer to the first computer when the second computer is to be authenticated (column 5: lines 2-14; column 6: lines 45-65; Figure 5: server challenge; Client DPC authentication challenge response);

transmit a response to the challenge from the first computer to the second computer (column 6: lines 55-65; column 7: lines 1-13; Figure 5: challenge response); and

verify the response with the second computer in order to authenticate and verify the computers (column 7: lines 30-40; Figure 5: Authentication response; DPC command response; success/Failure).

Kumar does not explicitly disclose credential based on a maximum iterative value security parameters. Funk in analogous art, however discloses, credential based on a maximum iterative value security parameters (column 4: lines 10-24; column 7: lines 37-42; column 18: lines 35-65). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Kumar to include credential based on a maximum iterative value security parameters. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide secure authentication against man in the middle attack for inner protocols that can generate encryption keys as suggested by Funk in (column 5: lines 25-33).

Kumar and Funk do not explicitly disclose credential based on an expiration time. Haverinen in analogous art, however discloses, credential based on an expiration time (0022; 0035; 0036). Therefore, it would have been obvious to a person having ordinary skill in the art at

the time the invention was made to modify the system disclosed by Kumar and Funk to include credential based on an expiration time This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide a strong authentication including Kerberos authentication service desirable in transactions involving confidential data as suggested by Haverinen (0002-0003).

As per claims 2 and 8:

Kumar and Funk do not explicitly disclose the challenge is a random number generated by the second computer computing device and the first computing device computes the response to the challenge by performing a predetermined function on the random number. Haverinen in analogous art, however discloses, the challenge is a random number generated by the second computer computing device and the first computing device computes the response to the challenge by performing a predetermined function on the random number (0041; 0042; challenge RAND; 0061: Preferably the challenge is a random code). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Kumar and Funk to include the challenge is a random number generated by the second computer computing device and the first computing device computes the response to the challenge by performing a predetermined function on the random number. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide a strong authentication including Kerberos authentication service desirable in transactions involving confidential data as suggested by Haverinen (0002-0003).

As per claims 3 and 9:

Haverinen discloses a method and a system, wherein the second computer computing device determines whether the first computer computing device response is valid by performing the predetermined function on the random number and comparing the result to the response (0182; 0201; 0203).

As per claims 4 and 10:

Haverinen discloses a method and a system, wherein the predetermined function is a hash function (column 6: lines 23-35).

As per claims 5 and 11:

Kumar discloses a method and a system, wherein the second computing device establishes a connection with the first computer computing device when the response is valid (Figure 6: DPC command and response; Success/Failure).

As per claim 49:

Kumar discloses a method for authenticating a computer, the method comprising the following steps:

issuing a credential based on session information, a hash seed, credential information from a first computing device to a second computer computing device (column 5: lines 2-14);

in response to a connection between the first computer and the second computer being terminated,

transmitting said credential and a computer challenge from the second computer to the first computer when the second computer is to be authenticated (column 5: lines 2-14; column 6: lines 45-65; Figure 5: server challenge; Client DPC authentication challenge response);

transmitting a response to said computer challenge from said first computer to said second computer (column 6: lines 55-65; column 7: lines 1-13; Figure 5: challenge response); and

verifying at said second computer whether said response is valid, wherein said second computer re-establishes a connection with the first computer when the response is valid (column 7: lines 30-40; Figure 5: Authentication response; DPC command response; success/Failure).

Kumar does not explicitly disclose credential based on a maximum iterative value security parameters. Funk in analogous art, however discloses, credential based on a maximum iterative value security parameters (column 4: lines 10-24; column 7: lines 37-42; column 18: lines 35-65). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Kumar to include credential based on a maximum iterative value security parameters. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide secure authentication against man in the middle attack for inner protocols that can generate encryption keys as suggested by Funk in (column 5: lines 25-33).

Kumar and Funk do not explicitly disclose credential based on an expiration time. Haverinen in analogous art, however discloses, credential based on an expiration time (0022;

0035; 0036). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Kumar and Funk to include credential based on an expiration time This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide a strong authentication including Kerberos authentication service desirable in transactions involving confidential data as suggested by Haverinen (0002-0003).

As per claims 50:

Kumar and Funk do not explicitly disclose the challenge comprises a random number generated by the second computer, wherein the first computer generates the response to the challenge by calculating a predetermined function of the random number, and wherein the second computer verifies whether the response is valid by calculating the predetermined function of the random number and comparing the result of the calculation to the response. Haverinen in analogous art, however discloses, the challenge comprises a random number generated by the second computer, wherein the first computer generates the response to the challenge by calculating a predetermined function of the random number, and wherein the second computer verifies whether the response is valid by calculating the predetermined function of the random number and comparing the result of the calculation to the response (0041; 0042; challenge RAND; 0061: Preferably the challenge is a random code). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Kumar and Funk to include the challenge comprises a random number generated by the second computer, wherein the first computer generates the response to the

challenge by calculating a predetermined function of the random number, and wherein the second computer verifies whether the response is valid by calculating the predetermined function of the random number and comparing the result of the calculation to the response. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide a strong authentication including Kerberos authentication service desirable in transactions involving confidential data as suggested by Haverinen (0002-0003).

As per claims 6, 12 and 51:

Haverinen discloses a method and system, wherein the first computer computing device determines whether the credential transmitted from the second computer computing device is valid by determining whether the expiration time of the credential has been exceeded (0035; 0036; expiration time; nonce random value).

Allowable Subject Matter

5. Claims 13-44 and 48 are allowed.

6. The following is an examiner's statement of reasons for allowance

Claims 13, 24, and 35 include the following features which are not taught or further suggested and would not have been obvious over prior arts of record and these features are:

issuing a credential based on session information, a hash seed, a maximum iterative value security parameters, credential information and an expiration time from a first computer to a

second computer; transmitting the credential and a generated first challenge from the second computer to the first computer;

determining with the first computer whether the credential is valid and computing a first response to the first challenge and a second challenge with the first computer and transmitting them to the second computer; determining with the second computer whether the first response is valid and computing a second response to the second challenge with the second computer; and transmitting them to the first computer; and

determining with the first computer whether the second response is valid to verify and authenticate the computers.

Claim 48 include the following features which are not taught or further suggested and would not have been obvious over prior arts of record and these features are:

issuing a credential based on session information, a hash seed, a maximum iterative value security parameters, credential information and an expiration time from the first user to the second user to authenticate them with a computer; and generating a first challenge with the second user; transmitting the credential and the first challenge to the first user;

determining with the first user whether the credential is valid and generating with the first user a first response to the first challenge and a second challenge and transmitting them to the second user; determining with the second user whether the first response is valid; generating with the second user a second response to the second challenge and transmitting the second response to the first user; and

determining with the first user whether the second response is valid in order to authenticate and verify the first and second users.

Conclusion

7. The prior arts made of record and not relied upon are considered pertinent to applicant's disclosure. See the notice of reference cited in form PTO-892 for additional prior arts.

Contact Information

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Techane J. Gergiso whose telephone number is (571) 272-3784 and fax number is **(571) 273-3784**. The examiner can normally be reached on between 9:00am - 6:00pm. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Techane J. Gergiso/

Examiner, Art Unit 2437